

REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1, 3-12, 14-17, 19-28 and 30-32 are pending in the application. Claims 1, 12, 17, and 28 are amended; and Claims 2, 13, 18, and 29 are canceled by the present amendment. Support for the amended claims can be found in the original specification, claims and drawings.¹ No new matter is presented.

In the outstanding Office Action, Claims 1-6, 16-22 and 32 were rejected under 35 U.S.C. § 102(b) as anticipated by Hind et al. (U.S. Patent No. 6,976,163, hereinafter Hind); Claims 12-15 and 28-31 were rejected under 35 U.S.C. § 102(b) as anticipated by Mattison (U.S. Patent No. 6,615,355); Claims 7-9 and 23-25 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hind in view of Sandler et al. (U.S. Patent No. 6,378,069, hereinafter Sandler); and Claims 10-11 and 26-27 were rejected under 35 U.S.C. § 103(a) as unpatentable over Hind in view Sandler and Arnold.

In response to the above noted rejections, Applicants respectfully submit that amended independent Claims 1, 12, 17 and 28 recite novel features clearly not taught or rendered obvious by the applied references.

Amended independent Claim 1 relates to an image forming apparatus that checks the authenticity of an update program. The apparatus includes a storing unit that stores a program operated by the apparatus and an acquiring unit that acquires an update program from an external source. The apparatus also includes an updating unit that determines whether an electronic signature of the update program is authentic, and updates the program stored in said storing unit using the acquired update program. Independent Claim 1 is further amended to recite, in part:

¹ E.g., specification, p. 21, lines 7-11.

wherein the authentication of the update program is performed based on a message digest of a configuration file of the update program *and a unique identification of the external source*.

Independent Claims 1, 12, 17 and 28, while directed to alternative embodiments, are amended to recite substantially similar features to those emphasized above. Accordingly, the remarks and arguments presented below are applicable to each of amended independent Claims 1, 12, 17 and 28.

Further, independent Claims 1, 12, 17 and 28 are amended to recite a subset of the features recited in dependent Claim 10. Specifically, dependent Claim 10 further clarifies, *inter alia*, that the electronic signature of the of the configuration file is generated by encrypting a message digest of the configuration file and identification information of the recording medium (e.g., external source).

In rejecting Claim 10, the outstanding Office Action admits that the proposed combination of Hind and Arnold fails to disclose that the “the encryption identification of the device” is used to perform the authentication of the update program. In an attempt to remedy this deficiency, the Office Action relies on Arnold and states that it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the cited references to arrive at this claimed feature. Applicants respectfully traverse this rejection and assert that amended independent Claims 1, 12, 17 and 28 recite novel features clearly not taught or rendered obvious by the applied references.

Arnold describes an apparatus and method for the secure distribution of data that encrypts a program and software updates using a private key of the data sender.² Arnold, however, fails to teach or suggest that *a unique identification of the external source* is included in his authentication information, whatsoever.

² Arnold, Abstract.

In addressing the features recited in dependent Claim 10, the Office Action relies on col. 7, lines 62-63, col. 8, line 1 and Fig. 3 and states that “the manufacturer computes a digital signature over the data D, and the data is encrypted using the symmetric key algorithm.” Thus, this cited portion of Arnold merely describes the use of a key generated by a manufacturer of the software to encrypt the software, but fails to teach or suggest that the data used to authenticate the update program includes *a unique identification of the external source ...from which the update program is acquired*, as recited in the pending independent claims.

As disclosed in an exemplary embodiment at p. 21, lines 8-20 of the specification, a serial number of a memory card, which acts as an external source of the update program, is a portion of the information used to authenticate a received update program. Thus, a unique identification (e.g., serial number) of the external source (e.g., memory card) from which the update program is acquired is used to authenticate the received update program.

In contrast, Arnold merely describes a process of using a software key generated by the developer of the software to facilitate a secure exchange of the software. At no point does Arnold teach or suggest using *a unique identification of the external source ...from which the update program is acquired* to authenticate a received software update, as recited in the amended independent claims.

Therefore, Hind, Sandler, and Arnold, neither alone, nor in combination, teach or suggest the above noted features recited in amended independent Claims 1 and 17. Accordingly, Applicants respectfully request that the rejection of independent Claims 1 and 17 (and the claims that depend therefrom) under both 35 U.S.C. § 102 and 35 U.S.C. § 103 be withdrawn.

Claims 12-15 and 28-31 were rejected under 35 U.S.C. § 102(b) as anticipated by Mattison. As noted above, independent Claims 12 and 28 are amended to recite substantially

similar features as those noted above with respect to independent Claims 1 and 17.

Applicants respectfully submit that Mattison fails to remedy the above noted deficiencies of the combination of Hind, Sandler, and Arnold.

Mattison describes system for providing the protection of flash memory containing a program from any unauthorized programming efforts.³ As described at col. 3, lines 25-33, a flash memory upgrade program containing a new flash memory image would be loaded into system main memory and executed. Then, at col. 3, lines 51-54, Mattison describes a process of comparing an original has value of the flash memory upgrade program with an independently generated hash value to find a match.

Thus, Mattison simply describes a process of authenticating a digital signature of an update program, but fails to teach or suggest incorporating any information unique to an *external source* of the software update into the authentication information. More specifically, Mattison fails to teach or suggest using *a unique identification of the external source ...from which the update program is acquired* to authenticate a received software update, as recited in the amended independent claims.

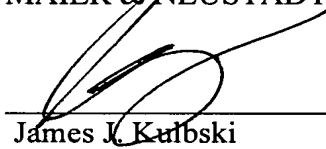
Accordingly, Applicants respectfully request that the rejection of independent Claims 12 and 28 (and the claims that depend therefrom) under 35 U.S.C. § 102(b) as anticipated by Mattison be withdrawn.

³ Mattison, Abstract.

Consequently, in view of the present amendment and in light of the foregoing comments, it is respectfully submitted that the invention defined by Claims 1, 3-5 and 47-50 is patentably distinguishing over the applied references. The present application is therefore believed to be in condition for formal allowance and an early and favorable consideration of the application is therefore requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



James J. Kulbski
Attorney of Record
Registration No. 34,648

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

Andrew T. Harry
Registration No. 56,959